10-12-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

·				
In re U.S. Patent Application of				
KAMINAGA et al.)			
Application Number: To be assigned)			
Filed: Concurrently herewith)			
-)			
For: TAMPER-RESISTANT MODULAR MULTIPLICATION METHOD)			

Honorable Assistant Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT

Sir:

Pursuant to 37 C.F.R. §§ 1.56 and 1.97, this Information Disclosure Statement is submitted in the above-identified patent application. A listing of documents to be published on the face of any patent granted from this application is submitted herewith on Form PTO-1449. Any other documents or information submitted for consideration by the Examiner are listed in this paper. A copy of each U.S. and foreign patent, or each publication or portion thereof listed or herein identified, is submitted herewith.

This Information Disclosure Statement is submitted with the initial application. Accordingly, no fee is due or payable at this time.

The Examiner is requested to acknowledge consideration of the information provided in this paper in accordance with prescribed procedures.

#2

Please charge any additional fees or credit any overpayments in connection with this paper to Deposit Account No. 08-1480.

Respectfully submitted,

Stanley P. Fisher

Registration Number 24,344

JUAN CARLOS A. MARQUEZ Registration No. 34,072

REED SMITH HAZEL & THOMAS LLP

3110 Fairview Park Drive Suite 1400 Falls Church, Virginia 22042 (703) 641-4200 August 24, 2001 For: The Patent Application

Our case No. NT0421US

* LIST OF THE PRIOR ART REFERENCES CITED IN THE SPECIFICATION

- 1. SMART CARD HAND BOOK (P.263)
- 2. Tamper Resistance a Cautionary Note (P.1~11)
- 3. Chinese Remaindering Based Cryptosystems in the Presence of Faults (P.1~5)
- 4. "Modular Multiplication Without Trial Division" By Peter L. Montgomery (P. 519~521)

Form PTO 1449				A'TTY. DOCKET NUMBER			L NUMBER O			
U.S. Department of Commerce				NITT.0028 Be Assigned						
Patent and Trademark Office Information Disclosure Statement by Applicant				KAMINAGA et al FILING DATE Concurrently Herewith			GROUP 966			
- Information 5				J.S. Patent I				Ü	,	
xaminer DOCUMENT Initial NUMBER		DATE		Name		CLASS	SUBC LASS	FILING DATE		
				Foreign Pa	atent Documents		<u> </u>			
Examiner	DOCUMENT NU	DOCUMENT NUMBER		NG DATE	Country	CLAS	SUB-	TRANS		
Initial						S	CLASS	YES	No	
	7						Ville I			
									<u></u>	
					g Author, Title, Da	te Pertinent	Pages, Etc.)			
	Ross Ander	Smart Card Handbook, pp. 263 Ross Anderson and Markus Kuhn, "Tamper Resistance A Cautionary Note", The Second USENI Workship on Electronic Commerce Proceedings, Oakland, California, Nov. 18-21, 1996, pp. 1-11								
	Marc Joye,	Arjen K	. Lenstra	a and Jean-J	acques Quisquater Journal of Cryptol	, "Chinese R ogy, pp. 1-5	temainderin	g Based Cry	ptosystems	
	Peter Mont Volume 44	gomery,	"Modul	ar Multipli	cation Without Tria	al Division",	Mathemati	cs of Compu	tation,	
								\		
l] l	1									

EXAMINER: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

DATE CONSIDERED

EXAMINER